CARE 1ST
HEALTH PLAN ARIZONA

ONECARE

Policy Name: Breach Notification Procedures of the HITECH/AARA of 2009	
Policy Number: 1107	Department: Compliance
Original Effective Date: 9/2013	Page(s): 10
Applies to ▪ AHCCCS ▪ DDD ▪ Medicare	

1.0 PURPOSE:

The purpose of this policy is to outline the internal processes, procedures, and time frames for reporting breaches of members/individuals' individually identifiable health information / personally identifiable information (PII) / protected health information (PHI) by Care1st Health Plan and ONECare by Care1st Health Plan Arizona, Inc. (HMO SNP) ("Care1st") and/or Care1st's contracted vendors and other related contracted entities pursuant to Section 13402 of the ARRA of 2009 / HITECH Act.

2.0 POLICY STATEMENT:

Following a breach of unsecured PHI covered entities (CEs), or Care1st, must provide notification of the breach to affected individuals, the Secretary, and, in certain circumstances, to the media. In addition, ARRA requires Business Associates contracted with Care1st to also notify Care1st of any discovered breaches of unsecured PHI.

3.0 AUTHORITIES AND REFERENCES:

- CMS Contract, Article IX (A)(2)
- AHCCCS Contract, Section D, Paragraph 62
- DDD Contract, Section 12.0
- Section 13402 of the Health Information Technology for Economic and Clinical Health (HITECH) Act
- CMS Memorandum dated December 16, 2008 – Security and Privacy Reminders and Clarification of Reporting Procedures
- CMS Memorandum dated September 28, 2010 – Update on Security and Privacy Breach Reporting Procedures
- Breach Notification Rule http://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html
- *HHS Guidance to Render Unsecured PHI Unusable, Unreadable, or Indecipherable to Unauthorized Individuals: http://www.hhs.gov/ hipaa/for-professionals/breach-notificationrule/guidance/index.html*

4.0 DEFINITIONS:

American Recovery & Reinvestment Act of 2009 (ARRA) – New HIPAA Notification Requirements on Breach of PHI. Section 13402 of ARRA requires HIPAA Covered Entities (CEs) to notify an individual if the CE discovers a breach of individual's unsecured PHI. Additionally, ARRA requires Business Associates (Bas) of CEs to notify the CEs of any discovered breaches of unsecured PHI. This requirement is only applicable in cases where the breach relates to "unsecured protected health information." If the breached PHI is secured, the notification requirements do not apply. (Refer to Section 10 *"Guidance to Render Unsecure PHI Unusable, Unreadable, or Indecipherable to Unauthorized Individuals"* beginning on page 4 of this document).

Breach – is presumed to be an impermissible use of disclosure of PHI under the Privacy Rule, unless Care1st or its Business Associate(s), as applicable, demonstrates that there is a low probability that the PHI has been comprised. Care1st determines a "low probability" based on at least a four-pronged risk analysis per the final Omnibus Rule (effective March 26, 2013).

- Three (3) Exceptions to the definition of "breach".
    - The first one applies to the unintentional acquisition, access, or use of PHI by a workforce member acting under the authority of a covered entity or Business Associate, and is not further used or disclosed in a manner not permitted by the Privacy Rule;
    - The second one applies to the inadvertent disclosure of PHI from a person authorized to access PHI at a covered entity or Business Associate to another person authorized to access PHI at the covered entity or Business Associate. In both cases, the information cannot be further used or disclosed in a manner not permitted by the Privacy Rule; and
    - The final exception to breach applies if the covered entity or Business Associate has a good faith belief that the unauthorized individual, to whom the impermissible disclosure was made, would not reasonably be able to retain the information.

CMS - the Centers for Medicare & Medicaid Services is the Federal agency that administers Medicare, Medicaid and the State Children's Health Insurance Program (SCHIP).

Personally Identifiable Information (PII) – any information about an individual including, but not limited to, education, financial transactions, medical history, and criminal or employment history, and information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, tec., including any other personal information, which is linked or linkable to an individual.

Protected Health Information (PHI) – any individual identifiable health information. Identifiable refers not only to the data that is explicitly linked to a particular individual (that's identified information). It also includes health information with data items which reasonable could be expected to allow individual identification.

Unsecured Protected Health Information – "Protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Security in the guidance issued under section 13402(h)(2) of Pub. L. 111-5." (45 CFR §164.402)

5.0 OPERATING PROTOCOL:

Internal Reporting:

1. When/if an attempted, suspected or successful breach incident is identified or committed by Care1st's staff and/or its first-tier and downstream entities; the incident is reported **immediately** to Care1st's Compliance and Information System (IS) Departments. The following individuals are immediately notified:

   The Director, Market Compliance Officer/Privacy Officer;
   The Director of IS; and
   Other Identified Individuals Involved in the breach, as deemed appropriate.
2. Log/Enter in the Compliance Database:

   The incident is logged in the Compliance database and is processed.

3. The Compliance and MIS Departments initiate the following risk assessment to determine whether the breach has a **low probability** of being compromised:
    a. Nature and extent of the PHI involved, including the types of identifiers and likelihood of re-identification;
    b. The unauthorized person who used the PHI or to whom the disclosure of PHI was made;
    c. Whether the PHI was actually viewed or acquired; and
    d. The extent to which the risk to the PHI has been mitigated

    Note that other factors may be considered when necessary.

4. Coordination with Other Departments Involved:

    The Director, Market Compliance Officer, and the Manager of MIS convenes and may obtain advice from its Corporate Legal Department and statements from appropriate individuals and departments involved in the breach incident.

    The Director, Market Compliance Officer, and the MIS Director and/or their designated representatives/staff assist, as appropriate, in reporting the incident to regulatory agencies following the steps, criteria, and time frames describe below.

5. Individual Notice:
    - Following discovery of a breach of unsecured PHI, Care1st notifies each individual whose unsecured PHI has been, or is reasonably believed by Care1st to have been accessed, acquired, used, or disclosed as a result of such breach.
    - A breach is treated as discovered by Care1st as of the first day on which such breach is known to Care1st, or, by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is a workforce member or agent of Care1st (as defined by common law).
        a. Written Notice:
        - Care1st notifies individuals in writing via first-class mail at the last known address of the individual or, if the individual agrees

to electronic notice and such agreement has not been withdrawn, by electronic mail.

- If Care1st is aware that the individual is deceased and has the address of the next of kin or personal representative, Care1st notifies next of kin or personal representative via first class mail.

b. Substitute Notice:

- If Care1st has insufficient or out-of-date contact information for 10 or more individuals, Care1st provides substitute individual notice by either posting the notice on the home page of Care1st's web site or by providing the notice in major print or broadcast media where the affected individuals likely reside
- If Care1st has insufficient or out-of-date contact information for fewer than 10 individuals, Care1st provides substitute notice by alternative form of written, telephone, or other means.

c. Additional notice in urgent situations:

- In any case deemed by Care1st to require urgency because of possible imminent misuse of secured PHI, Care1st may provide information to individuals by telephone or other means, as appropriate, in addition to providing written notice.

6. Time Frames for Notifications:

   a. Elements: Care1st provides notification without unreasonable delay and in no case later than 60 calendar days following the discovery of a breach and will include, to the extent possible:

      - A description of the breach;
      - A description of the types of information that were involved in the breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);
      - The steps affected individuals should take to protect themselves from potential harm as a result of the breach;
      - A brief description of what Care1st is doing to investigate the breach, mitigate the harm, and prevent further breaches, as well as Care1st's contact information; and

- For substitute notice provided via web posting or major print or broadcast media, the notification includes a toll-free number for individuals to contact Care1st to determine if members/individuals' PHI was involved in the breach. The toll-free number remains active for at least 90 days.

b. Plain language requirement: Care1st's notification is written in plain language.

7. Media Notice
For a breach affecting <u>more than 500 residents</u> of a State or jurisdiction area, in addition to notifying affected individuals, Care1st provides notice to prominent media outlets serving the State or jurisdiction (e.g., in the form of a press release). Similar to Individual Notice, Care1st provides this media notification without unreasonable delay and in no case later than 60 calendar days following the discovery of a breach and includes the same information required for the Individual Notice.

8. Notice to the Secretary of Department of Health & Human Services (DHHS):
In addition to notifying affected individuals and the media (where appropriate), Care1st notifies the Secretary of breaches of unsecured PHI. Care1st notifies the Secretary by visiting the DHHS web site and filling out and electronically submitting a breach report (Appendix A) at http://www.hhs.gov/hipaa/for-professionals/ /breach-notification/breach-reporting/index.html.

   - If a breach affects <u>500 or more individuals</u>, Care1st or its Business Associate notifies the Secretary without unreasonable delay and in no case later than 60 calendar days following a breach, unless a law enforcement official states to Care1st that such notice would impede a criminal investigation or cause damage to national security.
      1. If the law statement is in writing and specifies the time for which a delay is required, Care1st delays such notification or posting for the time period specified by law enforcement.
      2. If the statement is made orally, Care1st documents the statement, including the identity of the official making the statement, and delay the notification or posting temporarily and no longer than 30 days from the date of the oral

statement, unless a written statement is submitted during that time.

- If, however, a breach affects <u>fewer than 500 individuals</u>, Care1st notifies the Secretary of such breaches on an annual basis. Reports of breaches affecting fewer than 500 individuals are due to the Secretary no later than 60 calendar days after the end of the calendar year in which the breach is discovered.

9. Notification by a Care1st Business Associates (BAs):
   If a breach of unsecured PHI occurs at or by a Business Associate, the Business Associate notifies Care1st following the discovery of the breach. A breach is treated as discovered by a BA as of the first day on which such breach is known to the BA, or would have been known to the BA by exercising reasonable diligence. A BA is deemed to have knowledge of a breach if the breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is an employee, officer, or other agent of the BA.
   - The Business Associate must provide notice to Care1st without unreasonable delay and no later than 60 calendar days from the discovery of the breach, unless a law enforcement official states to the BA that such notice would impede a criminal investigation or cause damage to national security.
     - If the law statement is in writing and specifies the time for which a delay is required, Care1st delays such notification or posting for the time period specified by law enforcement
     - If the statement is made orally, Care1st documents the statement, including the identity of the official making the statement, and delay the notification or posting temporarily and no longer than 30 days from the date of the oral statement, unless a written statement is submitted during that time.
   - To the extent possible, the Business Associate provides Care1st with the identification of each individual affected by the breach as well as any information required to be provided by Care1st in its notification to affected individuals.
10. Burden of Proof:

Care1st and its Business Associates have the burden of proof to demonstrate that all required notifications have been provided or that a use or disclosure of unsecured PHI did not constitute a breach.

- Care1st applies all its existing Policies and Procedures related to Privacy Rule with respect to breach notification including, but not limited to:
  - o Reporting breach incidents to other regulatory agencies (e.g., Centers for Medicare & Medicaid Services (CMS)), as deemed required and/or appropriate;
  - o Sanctions against workforce members and/or contracted entities/vendors who did not comply with Care1st's procedures, as deemed appropriate; and
  - o Training of employees and/or contracted entities/vendors on Privacy and Security Rules

11. DHHS' Guidance to Render Unsecured PHI Unusable, Unreadable, or Indecipherable to Unauthorized Individuals:

    PHI is rendered unusable, unreadable, or indecipherable to unauthorized individuals if one ore more of the following applies:

    i. Electronic PHI has been encrypted as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without cause of a confidential process or key" (45 CFR 164.304 definition of encryption) and such confidential process or key that might enable the decryption has not been breached. To avoid a breach of the confidential process or key, these decryption tools should be stored on a device or at a location separate from the data they are used to encrypt or decrypt. The encryption processes identified below have been tested by the National Institute of Standards and Technology (NIST) and judged to meet this standard.

1. Valid encryption processes for data at rest are consistent with NIST Special Publication 800-111, Guide to Storage Encryption Technologies for End User Devices.[1]
2. Valid encryption processes for data in motion are those which comply, as appropriate, with NIST Special Publications 800-52, Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations; 800-77, Guide to Internet Protocol Security (IPsec) Virtual Private Networks (VPNs); or 800-113, Guide to Secure Socket Layer (SSL) VPNs, or others which are Federal Information Processing Standards (FIPS) 140-2 validated.

ii. The media on which the PHI is stored or recorded is destroyed in one of the following ways:

1. Paper, film, or other hard copy media have been shredded or destroyed such that the PHI cannot be read or otherwise cannot be reconstructed. Redaction is specifically excluded as a means of data destruction.
2. Electronic media have been cleared, purged or destroyed consistent with NIST Special Publication 800-88, Guidelines for Media Sanitization such that the PHI cannot be retrieved.

[1] NIST Roadmap plans include the development of security guidelines for enterprise-level storage devices, and such guidelines will be considered in updates of this guidance, when available.

CARE 1ST HEALTH PLAN ARIZONA

ONECARE

Policy Name: Breach Notification Procedures of the HITECH/AARA of 2009	
Policy Number: 1107	Department: Compliance
Original Effective Date: 9/2013	Page(s): 10

Applies to

- AHCCCS
- DDD
- Medicare

6.0 REVISION HISTORY:

Date	Reviewed/Revised By:	Reason for change
6/2017	Stacie Romney	Annual Review
06/2016	Crystal Cabrera	Revision
06/2015	Stephanie Miller	Annual Review
6/2014	Nizhoni Smith	Annual Review
9/2013	Nizhoni Smith	Policy Creation

7.0 CORPORATE APPROVAL:

Scott Cummings
State President

Deena Sigel
Vice President, Field Finance

Susan Cordier
Chief Operating Officer, State